



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,591	07/09/2007	Lior Golan	P-6325-US	3590
80048 7590 10/26/2010 Pearl Cohen Zedek Latzer, LLP 1500 Broadway 12th Floor New York, NY 10036				
EXAMINER				
GEORGANDELLIS, ANDREW C				
ART UNIT		PAPER NUMBER		
2453				
MAIL DATE		DELIVERY MODE		
10/26/2010		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/578,591

Applicant(s)

GOLAN ET AL.

Examiner

ANDREW GEORGANDELLIS

Art Unit

2453

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 May 2006.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 1-32 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 08 May 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/CIS-8)
Paper No(s)/Mail Date 5/8/2006, 10/23/2007

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____

DETAILED ACTION

Introduction

1. Claims 1-24 are pending. This Office Action is in response to Application 10/578,591 filed on 5/8/2006.

Claim Rejections: 35 U.S.C. 101

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. **Claims 1-7, 10, 14, 15, 17, 18, and 24-34 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.**

4. Claims 1-7, 10, 14, 15, 17, and 18 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory “process” under 35 U.S.C. 101 must (1) be tied to a particular machine, or (2) transform underlying subject matter to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The method including the step of “responding to a contact point, the response including a set of details, the set of details including a set of false personal information” ... is broad enough that the claim could be completely performed mentally, verbally, or without a machine.

5. Claims 24-34 recite a “system” that is not a process, machine, article of manufacture, or composition of matter. The claimed element “controller” is a non-structural limitation, and in light of the specification is disclosed as being software *per se*. Therefore, the claimed subject matter as a whole fails to fall within the definition of a process, machine, article of manufacture, or composition of matter.

Priority Claim

6. Applicant’s claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. However, the disclosure of the prior-filed application, provisional application No. 60/517,858, fails to provide adequate support or enablement in the manner provided by the first paragraph of 35 U.S.C. 112 for one or more claims of this application.

7. Specifically, the provisional application discloses that in response to a detected phishing attack, a service provider may perform “clogging: for example, the Phishing website which tries to collect data from the Service Provider’s customers, is filled with fake records of people, thus diluting the quality of data that the fraudsters obtain.” See pg. 7. In addition, the provisional application discloses “for example, the Phishing website which tries to collect data from the Service Provider’s customers is filled with fake records of people. When the Service Provider detects that these ‘fake people’ attempt to enter the Service Provider’s real website, the Service Provider can zero in an catch the fraudster...” See pg. 8.

8. However, the provisional application is silent as to the rate at which the responses are transmitted, the timing of the responses, the consistency of the personal information, the creation

and storage of false identities in a database, conducting the responses using multiple access points, intermediate networks and/or ISPs, generating a number of responses in proportion to the size of the attack (although the provisional application states that the size of an attack can be estimated, i.e., “the alert also may include an estimate of the size of the phishing scam.” See page. 7), marking a response using a cryptographic algorithm, and detecting the marking using a cryptographic key. In other words, Examiner can find no support in provisional application for claims 5-9, 11-13, 15, 17, 18, 20-23, 27-31, 33, and 34.

Claim Rejections: 35 U.S.C. 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

- 10. Claims 8, 23, and 30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**

11. Claims 8, 23, and 30 recite “a database including a set of false identities, each false identity including a set of data which is consistent within the set.” However, it is unclear whether “consistent within *the set*” refers to the “set of false identities” or the “set of data.”

Claim Rejections: 35 U.S.C. 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. Claims 1, 2, 3, 7, 9-13, 15, 24, 26, 29, and 31 are rejected under 35 U.S.C. 103(a) because they are unpatentable over Sweetchillisauc (NPL).

14. Regarding claims 1, 10, and 24, Sweetchillisauc teaches a method comprising: responding to a contact point created by a party committing fraud, the response including a set of details, the set of details including a set of false personal information (Sweetchillisauc teaches the concept of “scam baiting,” i.e., a form of Internet vigilantism where the vigilante (i.e., scam baiter) poses as a potential victim to the scammer in order to waste their time, gather information that will be of use to the authorities, or publicly humiliate the scammer. See http://en.wikipedia.org/wiki/Scam_baiting. Sweetchillisauc further teaches a request by a scammer (named “Stella Mike”) and a response to the request by a scam baiter (named “Kris Kringle”). The response includes various pieces of false personal information. For instance, the name “Kris Kringle” is an alias of “Santa Claus.” In addition, the address provided by “Kris Kringle” is “The Jolly Fatman Caravan and Camping Park.” Lastly, “Kris Kringle” provides a fake bank account, i.e., “Bank: St. Nicholas Bank Limited, Christmas Hills Branch, BSB Number: 039-884, Account Number: 4500-1276”).

15. Regarding claim 2, Sweetchillisauc teaches responding a plurality of times, each response including a different set of details (“Stella Mike” generates multiple requests directed to different individuals because generating multiple requests increases the likelihood that a potential victim will respond. Furthermore, each potential victim is potentially a scam baiter such

as “Kris Kringle.” Thus, “Stella Mike” receives multiple responses, each response being from a different scam baiter and therefore containing a different set of false personal information).

16. Regarding claims 4 and 26, Sweetchillisaucе teaches that the contact point is an e-mail address (The contact address of “Stella Mike” is “stellamike@mail.com”).

17. Regarding claims 7 and 29, Sweetchillisaucе teaches that each response includes a set of details that are internally consistent (The scam baiter attempts to fool the scammer into believing the response is genuine. Therefore, it may be inferred that the set of details in the response are internally consistent in order to make the response appear genuine).

18. Regarding claim 9, Sweetchillisaucе teaches that each response includes a set of details consistent with an Internet service provider used to respond (The responses include details regarding the service providers from which they originate. For instance, a response sent from ISP “America Online” is sent from the domain “aol.com”).

19. Regarding claims 11-13 and 31, Sweetchillisaucе teaches that the responding is conducted using a plurality of Internet access points and/or intermediate networks and/or Internet service providers (Scam requests are transmitted to multiple users all over the world in order to increase the likelihood of receiving a response. Thus, responses from scam baiters originate from all over the world and are therefore conducted using a variety of networks, access points, and ISPs).

20. Regarding claim 15, Sweetchillisaucе teaches that the number of responses is in proportion to a size of an attack in response to which the responses are sent (Each response is generated in response to a scam request. Therefore, the number of responses is correlated with

the number of requests. Thus, the greater the number of scam requests sent by “Stella Mike,” the greater the number of responses sent by scam baiters such as “Kris Kringle”).

21. Claims 3, 16, and 25 are rejected under 35 U.S.C. 103(a) because they are unpatentable over Sweetchillisauc, as applied to claims 1 and 24 above, in further view of Applicant Admitted Prior Art (AAPA).

22. Regarding claims 3, 16, and 25, Sweetchillisauc does not explicitly teach that the contact point comprises a website or responding comprises entering data into a web-form. However, AAPA teaches responding to a fishing attack that originates from a website by entering data into a web-form of the website. See Specification, pg. 2, par. 2.

23. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sweetchillisauc so that the responses are submitted by filling in a web-form because doing so allows the responses to be generated in response to a phishing attack originating from a website.

24. Claims 5, 6, 8, 18, 27, and 28 are rejected under 35 U.S.C. 103(a) because they are unpatentable over Sweetchillisauc, as applied to claims 1 and 24 above, in further view of Shraim (US 2005/0257261).

25. Regarding claims 5, 6, 27, and 28, Sweetchillisauc does not explicitly teach responding at a speed designed to mimic a human entering data in response to a phishing attack. However, Shraim teaches automatically generating a plurality of responses to a Phishing attack at a rate which can be varied depending upon the purpose of the responses. For instance, the responses can be generated at rate capable of overwhelming the attacker, or the responses can be generated at a rate intended to lead the attacker to believe that the responses are genuine. See pars. 92-96.

26. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sweetchillisauc so that responding comprises responding at a speed designed to mimic a human entering data in response to a phishing attack because doing so allows the responses to be automatically generated by a computer rather than manually generated by a human being. See also MPEP 2144.04.B.III, which states that “providing an automatic or mechanical means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art.”

27. Regarding claims 8 and 30, Sweetchillisauc and Shraim collectively teach creating a database including a set of false identities, each false identity including a set of data which is consistent with the set (Shraim teaches a safe data store 236, which stores personal information associated with one or more fictitious entities. See par. 23. See also fig. 2, item 236. It may be inferred that the personal information is internally consistent based on the fact that the personal information is used to fool an attacker).

28. Regarding claim 18, Sweetchillisauc and Shraim collectively teach that the timing of the sending of the data mimics the behavior of automated client software (Shraim teaches automatically generating a plurality of responses to a Phishing attack at a rate which can be varied depending upon the purpose of the responses. For instance, the responses can be generated at rate capable of overwhelming the attacker, or the responses can be generated at a rate intended to lead the attacker to believe that the responses are genuine. See pars. 92-96).

29. Claim 14 is rejected under 35 U.S.C. 103(a) because it is unpatentable over Sweetchillisauc, as applied to claim 1 above, in further view of Herz (US 2006/0053490).

30. Regarding claim 14, Sweetchillisaucе does not explicitly teach that the data in a response is marked, the method comprising monitoring an institution for the use of marked data in an attempted transaction. However, Herz teaches marking an account number or credit card number and monitoring use of the marked account number or credit card number to detect fraudulent use of the marked account number or credit card number. See par. 88.

31. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sweetchillisaucе so that account information included within the responses is marked because doing so would allow the marked account numbers to be used to capture scammers.

32. Claim 17 is rejected under 35 U.S.C. 103(a) because it is unpatentable over Sweetchillisaucе, as applied to claim 1 above, in further view of Shur (US 6,330,672).

33. Regarding claim 17, Sweetchillisaucе does not explicitly teach that response is marked using a cryptographic algorithm, such that the marking is detectable only with a suitable cryptographic key. However, Shur teaches inserting cryptographically hidden data into a data stream, such that the hidden data is detectable only via a cryptographic key. See col. 3, ln. 40-67.

34. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sweetchillisaucе.com to incorporate the above-described feature because doing so facilitates tracking of the marked response.

35. Claims 19, 22, and 32 are rejected under 35 U.S.C. 103(a) because they are unpatentable over Sweetchillisaucе in view of AAPA.

36. Regarding claims 19 and 32, Sweetchillisaucе teaches a method comprising contacting a contact point, the contact including a set of details, the set of details including a set of false

personal information (Sweetchillisaucе teaches the concept of “scam baiting,” i.e., a form of Internet vigilantism where the vigilante (i.e., scam baiter) poses as a potential victim to the scammer in order to waste their time, gather information that will be of use to the authorities, or publicly humiliate the scammer. See http://en.wikipedia.org/wiki/Scam_baiting. Sweetchillisaucе further teaches a request by a scammer (named “Stella Mike”) and a response to the request by a scam baiter (named “Kris Kringle”). The response includes various pieces of false personal information. For instance, the name “Kris Kringle” is an alias of “Santa Claus.” In addition, the address provided by “Kris Kringle” is “The Jolly Fatman Caravan and Camping Park.” Lastly, “Kris Kringle” provides a fake bank account, i.e., “Bank: St. Nicholas Bank Limited, Christmas Hills Branch, BSB Number: 039-884, Account Number: 4500-1276”).

37. However, Sweetchillisaucе does not explicitly teach that the contact point is a website, and that responding comprises entering data into a web-form. However, But teaches responding to a fishing attack that originates from a website by entering data into a web-form of the website. See Specification, pg. 2, par. 2.

38. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sweetchillisaucе so that the responses are submitted by filling in a web-form because doing so allows the responses to be generated in response to a phishing attack originating from a website.

39. Regarding claim 22, Sweetchillisaucе and AAPA collectively teach that each contact includes a set of details that are internally consistent (The scam baiter attempts to fool the scammer into believing the response is genuine. Therefore, it may be inferred that the set of details in the response are internally consistent in order to make the response appear genuine).

40. Claims 20, 21, 23, 33, and 34 are rejected under 35 U.S.C. 103(a) because they are unpatentable over Sweetchillisauc and AAPA, as applied to claims 19 and 32 above, in further view of Shraim.

41. Regarding claims 20, 21, and 34, Sweetchillisauc and AAPA do not explicitly teach responding at a speed designed to mimic a set of unrelated human users entering data in response to a phishing attack. However, Shraim teaches automatically generating a plurality of responses to a Phishing attack at a rate which can be varied depending upon the purpose of the responses. For instance, the responses can be generated at rate capable of overwhelming the attacker, or the responses can be generated at a rate intended to lead the attacker to believe that the responses are genuine. See pars. 92-96.

42. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sweetchillisauc/AAPA so that responses are generated at a rate designed to mimic a set of unrelated human users entering data in response to a phishing attack because doing so allows the responses to be automatically generated by a computer rather than manually generated by a human being. See also MPEP 2144.04.B.III, which states that “providing an automatic or mechanical means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art.”

43. Regarding claims 23, Sweetchillisauc, AAPA, and Shraim collectively teach creating a database including a set of false identities, each false identity including a set of data which is consistent with the set (Shraim teaches a safe data store 236, which stores personal information associated with one or more fictitious entities. See par. 23. See also fig. 2, item 236. It may be

inferred that the personal information is internally consistent based on the fact that the personal information is used to fool an attacker).

44. Regarding claim 33, Sweetchillisauc, AAPA, and Shraim collectively teach creating a database including a set of false identities (Shraim teaches a safe data store 236, which stores personal information associated with one or more fictitious entities. See par. 23. See also fig. 2, item 236).

Conclusion

45. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew Georgandellis whose telephone number is 571-270-3991. The examiner can normally be reached on Monday through Friday, 7:30-5:00 PM EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Krista Zele can be reached on 571-272-7288. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/578,591
Art Unit: 2453

Page 13

/ANDREW GEORGANDELLIS/
Examiner, Art Unit 2453

/Krista M. Zele/
Supervisory Patent Examiner, Art Unit 2453